¿Qué hacer si eres víctima de phishing?

Se desarrolló un programa con **90 cuentas online** personales «falsas». Una vez que las cuentas estuvieron activas, se llevaron a cabo distintas técnicas para llamar la atención de los ciberdelincuentes con el objetivo de rastrear sus actividades durante los siguientes nueve meses.

El informe desvelaba detalles sobre las técnicas y comportamientos de los hackers, incluyendo cuánto tiempo pasa desde que realizan el phishing hasta que acceden a la información de la víctima, qué busca el ciberdelincuente en la cuenta hackeada, qué señuelos llaman su atención y qué prácticas de seguridad emplean para esconder su rastro.

Algunos de los datos más llamativos del informe son, por ejemplo, el hecho de que los hackers buscan información relacionada con los negocios.

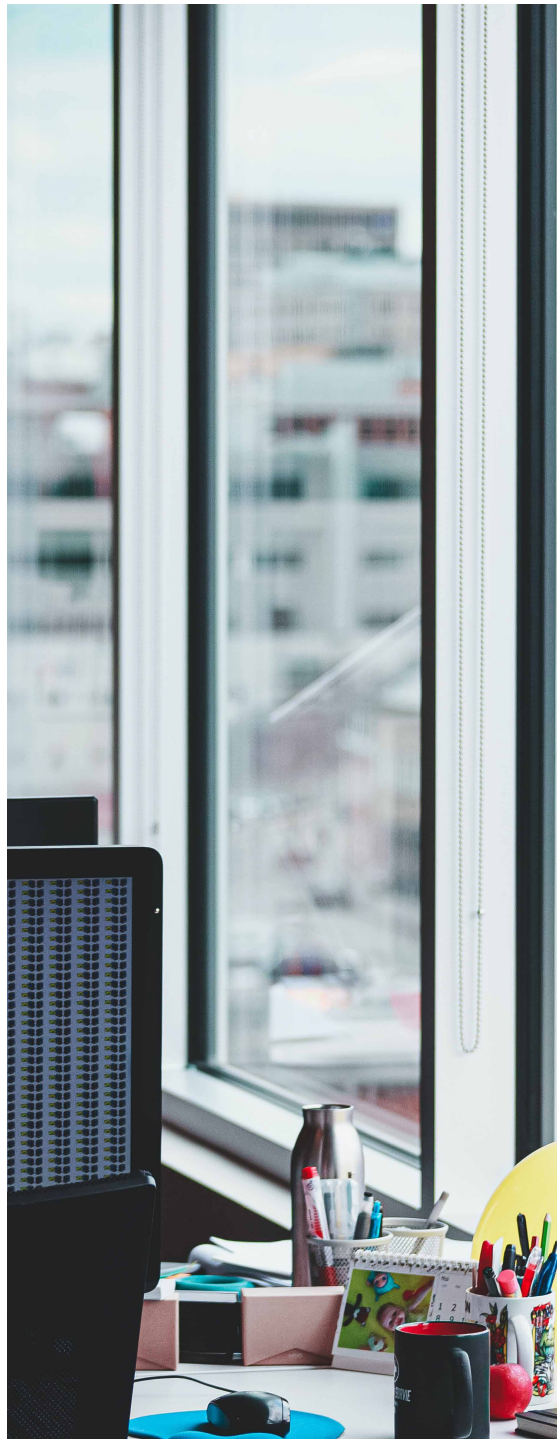
De hecho, el **25% de los phishers** leyeron emails en cuyos asuntos se mencionaban las palabras «datos financieros«, «base de datos de clientes» o «contacto de proveedor».

Más del 50% de las cuentas sufrieron accesos al menos **24 horas** después de que los hackers se hicieran con sus credenciales. Asimismo, los ciberatacantes accedieron en la mayoría de los casos de manera manual y no usando herramientas automáticas.

En un **74% de las incidencias,** las primeras alertas sucedieron en los siguientes 3 minutos después que que el hacker accediera a la cuenta, lo que indica que el hacker accedió a los «documentos-cebo» mientras exploraba la bandeja de entrada de la víctima.

Menos de las mitad de las falsas credenciales a las que los hackers accedieron fueron utilizadas, el estudio explique que posiblemente los hackers tienen acceso a tanta información que no cuenten con el tiempo suficiente para explorarla.

Además de los intentos de obtener información sensible de las cuentas hackeadas (la mayor parte de ella compuesta por contraseñas y números de tarjetas de crédito) los atacantes usaron estas cuentas para varias cosas: difundir campañas de phishing, scams relacionados con herencias, robo de contactos, peticiones de créditos y difusión de malware.



¿Cómo saber si eres víctima de phishing?

Si descubres que has sido objeto de un ciberataque del tipo phishing en un lapso relativamente corto de tiempo, puedes intentar minimizar el daño accediendo a tu cuenta (si es posible) para expulsar al hacker de la misma: cambia la contraseña y comprueba si el atacante ha cambiado cualquiera de las settings o configuraciones de tu cuenta para asegurarse de seguir teniendo acceso a la misma en caso de que modificaras la contraseña. Revisar por ejemplo si ha indicado una dirección secundaria de recuperación de contraseña, reenvío de emails a otra dirección, etc.

Si no tienes la seguridad completa respecto a si el atacante ha accedido a tu cuenta, puedes comprobar estas tres señales para cerciorarte:

1 Presencia de notificaciones del tipo «Nuevo aviso de inicio de sesión» en la «Papelera». Sólo el 2% de los atacantes, según el informe, borró de manera permanente el email con la alerta de nuevo inicio de sesión.

2 Si tu proveedor de correo electrónico ofrece un registro de actividad, compruébalo para ver si se han realizado acciones repetidas para marcar los mensajes como «no leídos».

3 Comprueba la carpeta de mensajes enviados para determinar si hay algún mensaje que te llama la atención. También revisa la «papelera» para descubrir notificaciones de «delivery failure». Durante la investigación, sólo el 13% de los atacantes borraron de manera permanente este tipo de mensajes.

Fuente de información:
cybersecuritynews